Bydgoscy Lekarze spółka z ograniczoną odpowiedzialnością

z siedzibą w Bydgoszczy

ul. Małeckiego 5

85 – 472 Bydgoszcz

KRS 0000955323

NIP 9671453472

POLITYKA OCHRONY DANYCH OSOBOWYCH
Zasady ogólne

Spis treści

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1. Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem Danych Osobowych i w sprawie swobodnego przepływu takich Danych oraz uchylenia dyrektywy 95/46/WE (dalej jako RODO),
2. Ustawą z dnia 10 maja 2018 o ochronie danych osobowych (dalej jako Ustawa).

Administratorem danych osobowych jest spółka działająca pod firmą Bydgoscy Lekarze spółka z ograniczoną odpowiedzialnością z siedzibą w Bydgoszczy (85-472), przy ul. Małeckiego 5, NIP 9671453472, wpisana do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod nr KRS 0000955323 (dalej jako: Administrator, AD lub Jednostka).

W skład obowiązującej u AD **Polityki ochrony danych osobowych,** regulującej zasady przetwarzania danych osobowych w Spółce wchodzą:

1. niniejsze Zasady ogólne,
2. Procedury bezpieczeństwa,
3. Raport z szacowania ryzyka i doboru środków bezpieczeństwa.

Polityka bezpieczeństwa ochrony danych osobowych reguluje zasady przetwarzania danych osobowych przez Administratora. Wszystkie informacje gromadzone przez Administratora podczas wykonywania standardowych działań, w tym dane osobowe, są niezbędne do prowadzenia działalności i uczestnictwa w obrocie, konieczne jest zatem zapewnienie ich należytej ochrony, w tym zwłaszcza poprzez wielowątkową, systematyczną edukację użytkowników.

Realizacja zadań wynikających z RODO i Ustawy wymaga między innymi efektywnego dostępu do informacji zawierających dane osobowe oraz zapewnienia odpowiedniego poziomu bezpieczeństwa tych danych. Utrata poufności, integralności, dostępności, autentyczności lub niezawodności będzie miała negatywny wpływ tak na bieżącą działalność, jak i wizerunek Administratora. Bezpieczeństwo danych osobowych oznacza ich ochronę przed szerokim spektrum zagrożeń w celu zachowania poufności, integralności i dostępności informacji, a także minimalizacji ryzyka oraz zapewnienia ciągłości działania Administratora i realizacji przedmiotu jego działalności na odpowiednim poziomie. Bezpieczeństwo informacji można osiągnąć zapewniając jednocześnie odpowiednią infrastrukturę, sprzęt i stosowne oprogramowanie z jednej strony, z drugiej zaś - wdrażając odpowiedni zestaw zabezpieczeń organizacyjnych, czego dotyczy niniejsza Polityka bezpieczeństwa. **Polityka bezpieczeństwa jest więc zbiorem zasad i procedur, którym muszą podporządkować się wszystkie osoby posiadające dostęp do danych osobowych przetwarzanych przez Administratora, bez względu na status zatrudnienia (umowa o pracę, umowa cywilnoprawna, stażyści, praktykanci). Zasady i procedury opisane w niniejszej Polityce bezpieczeństwa obowiązują we wszystkich miejscach prowadzenia działalności przez Administratora.**

Administrator oraz działające z jego upoważnienia osoby, dokładają szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, mając przy tym na względzie, iż konieczne jest wykazanie przestrzegania RODO i Ustawy („**rozliczalność**"). W szczególności Administrator zapewnia, że dane osobowe są:

1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane te dotyczą („**zgodność z prawem, rzetelność i przejrzystość**"),
2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („**ograniczenie celu**"),
3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („**minimalizacja danych**"),
4. prawidłowe i w razie potrzeby uaktualniane („**prawidłowość**"),
5. przechowywane w formie umożliwiającej identyfikację osoby, której dane te dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Wyjątkowo dane osobowe będą mogły być przechowywane przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych („**ograniczenie przechowywania**"),
6. przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, („**integralność i poufność**").

Opisane w Polityce procedury dotyczące ochrony danych osobowych, mają zastosowanie zarówno do przetwarzania danych osobowych w formie elektronicznej, jak i papierowej, w sposób całkowicie lub częściowo zautomatyzowany i w sposób inny niż zautomatyzowany, danych stanowiących część zbioru lub mających stanowić część zbioru danych.

Dane osobowe przetwarzane są w celu:

1) realizacji statutowych zadań i obowiązków Administratora,
2) zapewnienia prawidłowej, zgodnej z prawem polityki personalnej i bieżącej obsługi stosunków pracy, a także innych stosunków zatrudnienia nawiązywanych jako pracodawca i zleceniodawca,
3) realizacji innych usprawiedliwionych celów i zadań Administratora z poszanowaniem praw i wolności osób powierzających AD swoje dane osobowe.

Podstawowe definicje

1) „**Dane osobowe**" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osoba, której dane dotyczą). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

2) **„Przetwarzanie**" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie,

usuwanie lub niszczenie, które można podzielić na dwie grupy:

3) **„Ograniczenie przetwarzania”** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

4) **„Profilowanie”** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

5) **„Pseudonimizacja”** oznacza przetworzenie danych osobowych w taki sposób, by bez użycia dodatkowych informacji nie można ich było już przypisać konkretnej osobie, pod warunkiem jednak, że takie dodatkowe informacje są przechowywane osobno i są należycie zabezpieczone.

6) **„Zbiór danych”** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

7) **„Administrator danych”** (też Administrator, AD) oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W rozumieniu niniejszej Polityki Administratorem danych jest Bydgoscy Lekarze sp. z o.o. z siedzibą w Bydgoszczy.

8) **Inspektor Ochrony Danych (IOD)** – oznacza osobę powołaną przez Administratora na podstawie kwalifikacji i doświadczenia kontrolującą przestrzeganie procedur w zakresie danych osobowych i zgłoszoną do Prezesa Urzędu Ochrony Danych.

9) **Administrator Systemu Informatycznego (ASI) / Informatyk** – oznacza wyznaczonego pracownika lub podmiot zewnętrzny, realizującego obsługę IT Administratora, odpowiedzialnego za realizację zadań związanych z zarządzaniem systemem informatycznym, w tym za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów infrastruktury informatycznej oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, a także ich utratą.

10) **„Podmiot przetwarzający"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

11) **„Odbiorca"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest Stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców.

12) **„Strona trzecia"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, Administrator, podmiot przetwarzający czy osoby, które – z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

13) **„Zgoda osoby, której dane dotyczą**" oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli (w formie oświadczenia lub wyraźnego działania potwierdzającego), którym osoba, której dane dotyczą, przyzwala na przetwarzanie dotyczących jej danych osobowych.

14) **„Naruszenie ochrony danych osobowych"** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

15) **„Dane genetyczne"** oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.

16) **„Dane biometryczne"** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

17) **„Dane dotyczące zdrowia"** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym

osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

18) „**Przedstawiciel**" oznacza osobę fizyczną lub prawną, która została wyznaczona na piśmie przez Administratora lub podmiot przetwarzający do reprezentowania Administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z przepisów prawa o ochronie danych osobowych.

19) „**Przedsiębiorca**" oznacza osobę fizyczną, prawną lub jednostkę organizacyjną prowadzącą działalność gospodarczą, niezależnie od formy prawnej.

20) **„Pracownik"** oznacza osobę fizyczną pozostającą z Administratorem w stosunku pracy, osobę fizyczną w stosunku do której Administrator występuje jako pracodawca – użytkownik, a także osobę fizyczną świadczącą na rzecz Administratora usługi z wykorzystaniem sprzętu i infrastruktury należącej do Administratora na podstawie innej umowy.

21) **„Organ nadzorczy"** oznacza Prezesa Urzędu Ochrony Danych Osobowych.

22) **System teleinformatyczny (TI, IT)** - zespół współpracujących ze sobą według określonych reguł urządzeń, oprogramowania, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

23) **Dostępność** - właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.

24) **Poufność** - właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym podmiotom.

25) **Ryzyko** - prawdopodobieństwo, że określone zagrożenie w połączeniu z podatnością na to zagrożenie doprowadzi do utraty lub zniszczenia zasobów.

26) **Integralność** - właściwość polegająca na zapewnieniu dokładności i kompletności aktywów.

27) **Autentyczność** - właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji).

28) **Niezaprzeczalność** - właściwość oznaczająca niemożność wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów.

Cel polityki ochrony Danych Osobowych

Celem wprowadzenia niniejszej Polityki jest:

1) ochrona danych osobowych przetwarzanych i gromadzonych w Jednostce w zakresie:

a) zabezpieczenia przed dostępem do danych przez osoby nieupoważnione, na każdym etapie przetwarzania tych danych, w tym wprowadzania, aktualizacji lub usuwania, wyświetlania lub drukowania zestawień i raportów, przemieszczania danych w sieci lokalnej pomiędzy programami i osobami je przetwarzającymi,
b) metod archiwizacji oraz ochrony danych zarchiwizowanych na nośnikach zewnętrznych i wydrukach,
c) procedur niszczenia niepotrzebnych wydruków lub nośników z danymi,
d) ustalenia i wdrożenia zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia gromadzące i przetwarzające dane,
e) określenia polityki i sposobów dostępu do tych pomieszczeń przez pracowników, personel pomocniczy oraz serwis zewnętrzny,

2) zmniejszenie ryzyka utraty danych,
3) określenie zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych,
4) podnoszenie świadomości pracowników i ich pełne zaangażowanie w ochronę przetwarzanych danych.

Procedury określone przez niniejszy dokument mają zastosowanie do całego systemu przetwarzania danych osobowych, w tym do wszystkich komputerów, na których przetwarzane są dane osobowe, a w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których są lub będą przetwarzane dane osobowe,
2) wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się dane osobowe,
3) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane dane osobowe,
4) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów, praktykantów i innych osób mających dostęp do informacji podlegających ochronie (w tym osób zatrudnionych na podstawie umowy prawa cywilnego).

<u>Sposób i zakres udostępniania dokumentu.</u>

1) Wszyscy pracownicy, a w szczególności osoby upoważnione do przetwarzania danych osobowych w zbiorach i bazach danych prowadzonych w Jednostce są zobowiązani zapoznać się z niniejszym dokumentem.
2) Za rozpowszechnienie dokumentu i umożliwienie zapoznania się z nim przez wszystkich pracowników odpowiedzialny jest Administrator.
3) Dokument dostępny będzie w formie elektronicznej oraz papierowej.

Obowiązkiem wszystkich pracowników jest przestrzeganie szczegółowych zasad postępowania opisanych w Polityce.

ORGANIZACJA SYSTEMU BEZPIECZEŃSTWA DANYCH OSOBOWYCH.
ZAKRESY OBOWIĄZKÓW

Za organizację systemu ochrony danych osobowych odpowiada Administrator danych, który wdrożył na podstawie analizy ryzyka naruszenia przepisów o ochronie danych osobowych i naruszenia praw i wolności osób fizycznych, których dane przetwarza, odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z prawem.

Administrator danych (oraz podmiot przetwarzający) wyznacza Inspektora Ochrony Danych zawsze gdy:

1. przetwarzania dokonują organ lub podmiot publiczny,
2. główna działalność Administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę lub
3. główna działalność Administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę danych wrażliwych (szczególnych kategorii) lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Inspektor Ochrony Danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań.
Administrator (podmiot przetwarzający) publikują dane kontaktowe Inspektora Ochrony Danych i zawiadamiają o nich organ nadzorczy – Prezesa Urzędu Ochrony Danych Osobowych

Zakresy obowiązków osób odpowiedzialnych za bezpieczeństwo Danych Osobowych.

<u>1.Administrator danych.</u>
Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, Administrator wdraża odpowiednie środki techniczne i organizacyjne. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
W szczególności:

1. opracowuje i wdraża Politykę Ochrony Danych Osobowych,
2. wyznacza Inspektora Ochrony Danych,
3. zatwierdza Raport z analizy ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania,
4. wdraża odpowiednie środki techniczne i organizacyjne, by spełnić wymogi prawa w zakresie ochrony danych osobowych oraz chronić prawa osób, których dane dotyczą,
5. prowadzi rejestr czynności przetwarzania danych osobowych.

<u>2. Inspektor Ochrony Danych.</u>

Inspektor Ochrony Danych podlega bezpośrednio Administratorowi danych.
Ma następujące zadania:

1. informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich zgodnie z prawem oraz zatwierdzoną Polityką ochrony danych osobowych i doradzanie im w tej sprawie,
2. monitorowanie przestrzegania przepisów prawa oraz Polityki ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
3. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonywania,
4. współpraca z organem nadzorczym,
5. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych.

Ponadto Inspektor Ochrony Danych

1. nadzoruje za pośrednictwem Administratora systemu informatycznego przestrzeganie zasad ochrony danych osobowych w systemie teleinformatycznym, w tym właściwego i bezpiecznego obiegu dokumentów oraz elektronicznych nośników informacji zawierających dane osobowe,
2. może wydawać w imieniu i z upoważnienia Administratora Danych upoważnienia do przetwarzania Danych Osobowych,
3. monitoruje Rejestr czynności przetwarzania danych osobowych, na podstawie danych przekazywanych przez Administratora,
4. nadzoruje za pośrednictwem osób funkcyjnych zapewnienie bezpieczeństwa fizycznego obszaru przetwarzania danych osobowych;
5. nadzoruje za pośrednictwem Administratora systemu informatycznego zapewnienie dostępu do systemu teleinformatycznego (TI) wyłącznie upoważnionym osobom, posiadającym odpowiednie upoważnienie dostępu do danych osobowych,
6. uczestniczy w opracowywaniu projektów dokumentów normatywnych regulujących w Jednostce problematykę ochrony danych osobowych.

3. Administrator systemu informatycznego (ASI)

ASI – jest to osoba wyznaczona przez Administratora danych osobowych spośród pracowników lub spoza ich grona. Podlega Administratorowi danych i współpracuje w zakresie przestrzegania procedur w zakresie przetwarzania danych osobowych w systemach teleinformatycznych.
ASI realizuje zadania w zakresie zapewnienia funkcjonowania oraz przestrzegania zasad bezpieczeństwa systemu IT przetwarzającego dane osobowe, a w szczególności:

1. koordynuje zadania osób administrujących poszczególnymi systemami informatycznymi,
2. odpowiada za obsługę techniczną systemu IT przetwarzającego dane osobowe,
3. odpowiada za konfigurację systemu operacyjnego zainstalowanego na komputerach zgodnie z zaleceniami,

4. aktualizuje oprogramowanie antywirusowe,
5. nadaje uprawnienia do dostępu do zbiorów danych przetwarzanych w systemie IT zgodnie ze wskazaniami AD,
6. prowadzi ewidencję upoważnień do przetwarzania danych osobowych,
7. nadzoruje pracę uprawnionych użytkowników przetwarzających dane osobowe w systemie IT,
8. uczestniczy w opracowywaniu projektów wymagań bezpieczeństwa dla systemów przetwarzających dane osobowe oraz nadzoruje przestrzeganie wymagań przez uprawnionych użytkowników,
9. niezwłocznie informuje Inspektora Ochrony Danych o stwierdzonych naruszeniach bezpieczeństwa systemu teleinformatycznego,
10. proponuje wprowadzenie zmian mających na celu poprawę bezpieczeństwa systemu teleinformatycznego.

Ponadto ASI:

11. utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu IT do przetwarzania danych osobowych i nadanych indywidualnych identyfikatorów dostępu do systemu IT,
12. upewnia się, czy cały personel posiadający dostęp do systemu IT posiada stosowne upoważnienia dostępu do przetwarzania danych osobowych,
13. prowadzi osobiście profilaktykę antywirusową systemu TI,
14. dokonuje wraz z Inspektorem Ochrony Danych analizy zgłoszonych przypadków incydentów infekcji wirusowych lub innych, wskazujących na nieautoryzowane próby ingerencji w systemie bezpieczeństwa oraz, w zależności od stopnia zagrożenia funkcjonowania systemu bezpieczeństwa, podejmuje odpowiednie kroki zaradcze zapewnienie strategii, uregulowań i procedur bezpieczeństwa,
15. prowadzi szkolenia dla użytkowników z zakresu bezpieczeństwa teleinformatycznego i przestrzegania wymagań bezpieczeństwa,
16. wykonuje archiwizację danych systemu IT, zgodnie z obowiązującymi procedurami,
17. uczestniczy w analizie ryzyka i informuje Inspektora Ochrony Danych o wszelkich lukach naruszeniach i zagrożeniach,
18. analizuje rejestr zdarzeń (logi systemowe).

UWAGA: w przypadku, gdy Administrator nie powoła Administratora Systemu Informatycznego, obowiązki przewidziane w powyższej sekcji realizuje inna osoba wyznaczona przez Administratora.

4. Użytkownik systemu przetwarzania danych osobowych – każdy pracownik, który wykonując czynności służbowe, przetwarza dane osobowe, tzn. wykonuje na nich operacje takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie niezależnie czy odbywa się to w zbiorach tradycyjnych czy systemie TI.

Użytkownicy systemu są odpowiedzialni za zapewnienie bezpieczeństwa danych osobowych, w tym danych przetwarzanych w systemie IT, a w szczególności są zobowiązani do:

1. zapoznania się z Polityką ochrony danych osobowych i przestrzegania jej procedur,
2. utrzymania poufności swoich haseł dostępu do systemu TI oraz przestrzegania ustalonych reguł złożoności przy zmianie hasła,
3. zgłaszania Inspektorowi Ochrony Danych oraz Administratorowi faktycznych i potencjalnych incydentów w obszarze ochrony danych osobowych,
4. przeprowadzania kontroli antywirusowej wykorzystywanych elektronicznych nośników informacji,
5. sporządzania kopii zapasowych zbiorów danych, za których administrowanie są odpowiedzialni.

ZGODNOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH Z PRAWEM

Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków, tzn. istnieje prawna podstawa dla tego przetwarzania:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze,
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej,
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

PRZETWARZANIE SZCZEGÓLNYCH KATEGORII DANYCH OSOBOWYCH

1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych, w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
2. Powyższe nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:
   a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach,

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,
c) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego,
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,
f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy.

WARUNKI WYRAŻENIA ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

1. Jeżeli przetwarzanie odbywa się na podstawie zgody, Administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
2. Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, musi zostać o tym poinformowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.
5. W przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 13 lat i wyraziło zgodę na to przetwarzanie. Jeżeli dziecko nie ukończyło 13 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

OBOWIĄZKI INFORMACYJNE ADMINISTRATORA DANYCH

Informacje o przetwarzaniu danych osobowych

1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności, gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji o przetwarzaniu danych osobowych. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
2. Administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z prawem dostępu do danych osobowych. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.
3. Jeżeli Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.
4. Jeżeli Administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie dotyczące przetwarzania jej danych osobowych, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

1. Jeżeli dane osobowe zbierane są od osoby, której dotyczą, Administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:
    a) swoją tożsamość i dane kontaktowe oraz gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela,
    b) gdy ma to zastosowanie – dane kontaktowe Inspektora Ochrony Danych,
    c) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania,
    d) prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią – o ile ma to zastosowanie,
    e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
    f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

2. Podczas pozyskiwania danych osobowych Administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:
    a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
    b) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
    c) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
    d) informacje o prawie wniesienia skargi do organu nadzorczego,
    e) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
    f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.
3. Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.
4. Powyższe zasady informacyjne nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą.

1. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, Administrator podaje osobie, której dane dotyczą, następujące informacje:
    a) swoją tożsamość i dane kontaktowe oraz gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela,
    b) gdy ma to zastosowanie – dane kontaktowe Inspektora Ochrony Danych,
    c) cele przetwarzania, do których mają posłużyć dane osobowe oraz podstawę prawną ich przetwarzania,
    d) kategorie odnośnych danych osobowych,
    e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
    f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej.
2. Ponadto, Administrator podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą:
    a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,

b) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
c) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
d) informacje o prawie wniesienia skargi do organu nadzorczego;
e) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych,
f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

3. Informacje powyższe, Administrator podaje:
   a) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych,
   b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą lub
   c) jeżeli planuje się ujawnić dane Osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
4. Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.
5. Powyższe nie ma zastosowania, gdy – i w zakresie, w jakim:
   a) osoba, której dane dotyczą, dysponuje już tymi informacjami,
   b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. W takich przypadkach Administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której Dane dotyczą, w tym udostępnia informacje publicznie.

Podmiot przetwarzający

1. Jeżeli przetwarzanie ma być dokonywane w imieniu Administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszej polityki i przepisów prawa i chroniło prawa osób, których dane dotyczą.
2. Podmiot przetwarzający nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
3. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy, określającej przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj

danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa Administratora.

4. Umowa określa w szczególności, że podmiot przetwarzający:
   a. przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora,
   b. zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności przetwarzanych danych,
   c. podejmuje wszelkie środki bezpieczeństwa przetwarzania wymagane na mocy art. 32 RODO,
   d. po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie,
   e. udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków prawnych oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

NARUSZENIE OCHRONY DANYCH OSOBOWYCH

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki, **nie później niż w terminie 72 godzin** po stwierdzeniu naruszenia, zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Zgłoszenie musi zawierać:

a. charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
b. imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
c. możliwe konsekwencje naruszenia ochrony danych osobowych,
d. opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi.

Dokumentowanie naruszenia ochrony danych osobowych.

Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania obowiązków w związku z wystąpieniem incydentu.
Po przeprowadzeniu postępowania wyjaśniającego oraz działań korygujących lub zapobiegawczych dokonywana jest ocena efektywności ich zastosowania oraz ponowna analiza ryzyka.